

REMARKS

Reconsideration of the above-identified application in view of the amendments above and the remarks following is respectfully requested.

Claims 1-36 are currently pending.

Claims 1-30 are rejected under 35 USC § 102(b).

Claims 9-16 and 31-36 are rejected under 35 USC § 103(a).

In reply, Applicant has amended Claims 1, 18, 19, 21, 24, 26, and 31, and has added new Claims 37-42. It is submitted that no new subject matter has been added by these amendments, and that support therefor may be found in the application, for example, at page 23, lines 11, 15, and 30; page 24, line 5, and page 35, line 16.

Claim Rejections – 35 USC § 102

In this section of the Office Action, Claims 1-30 were rejected under 35 USC § 102 (b) as being unpatentable over Atkinson (US Patent No. 5,511,122). Applicant respectfully traverses this rejection.

In response and in view of the amendments to Claims 1, 18, 19, 21, 24, and 26, it is submitted that there is no prima facie basis for the Examiner's assertion that these claims are anticipated by the teachings of Atkinson, as will be discussed below.

Atkinson teaches a method for network authentication of a host whereby a sending host (hostA) is verified by a receiving host (hostB) or by an intermediate router or gateway, such that "host b will...verify the authenticity of hostA." As discussed in detail in the patent (column 9, line 36; and column 10, line 8), data provided by hostA may be decoded by hostB, in order to verify the authenticity of hostA. This is shown in the appended fig. 3, at ref. nos. 16' and 88. In the case of intermediate authentication (column 11, lines 10 and 62), data provided by hostA is utilized by an intermediate router, as well as by hostB, to verify the authenticity of hostA. This is shown in the appended fig. 4, at ref. nos. 16, 106, and 124. Atkinson does not teach verifying the authenticity of a user.

In contrast, amended Claim 1 recites "A method of authenticating, using an authentication server, the use of an authentication device by at least a first user over a communication network via an intermediate communication device, comprising: receiving an authentication datagram by said intermediate device, said authentication datagram including

data from the first user; protecting said datagram by said intermediate device, by at least one of changing, adding to, encrypting and signing of said datagram; and forwarding said datagram to said authentication server for authentication of the first user."

Also in contrast to the teachings of Atkinson, amended Claim 18 recites "A method for authentication of the vendor."

Further in contrast to the teachings of Atkinson, amended Claim 19 recites "A method including "outputting said validation answer for authentication of the first user."

Yet further in contrast to the teachings of Atkinson, amended Claim 21 recites "A method of generating a code set for a remote authentication device, said remote device configured for authentication of at least a first user."

Yet further in contrast to the teachings of Atkinson, amended Claim 24 recites "A method of communication between a vendor and a user using an authentication device," including "authentication of the vendor..." and "...authentication of the user."

Yet further in contrast to the teachings of Atkinson, amended Claim 26 recites "A method of remote validation of at least a first user," including "outputting a validation signal for the first user."

In light of the above, it is submitted that amended independent Claims 1, 18, 19, 21, 24, and 26 are not anticipated by Atkinson and are, therefore, allowable. It is further submitted that Claims 2-17, 20, 22-23, 25, and 27-30 are allowable, as they depend from allowable claims.

Claim Rejections – 35 USC § 103

In this section of the Office Action, Claims 9-16 and 31-36 were rejected under 35 USC § 103 (a) as being unpatentable over Atkinson in view of Daudelin (US Patent No. 4,716,376). Applicant respectfully traverses this rejection.

It is submitted that there is no prima facie basis for the Examiner's assertion that these claims are unpatentable, as will be discussed below.

Neither Atkinson nor Daudelin teaches the limitations found in amended independent Claim 1, namely, "A method of authenticating, using an authentication server, the use of an authentication device by at least a first user over a communication network via an intermediate communication device, comprising: receiving an authentication datagram by said intermediate device, said authentication datagram including data from the first user; protecting said datagram by said intermediate device, by at least one of changing, adding to,

encrypting and signing of said datagram; and forwarding said datagram to said authentication server for authentication of the first user."

Additionally, neither Atkinson nor Daudelin teaches the limitation found in amended independent Claim 31, namely, "A method of detecting a transmission of an acoustic multitone Frequency Shift Key (FSK) signal from at least a first user comprising: receiving an acoustic signal from said at least a first user; converting the signal into a Hilbert-transform representation of the signal; correlating said converted signal with at least one reference signal representing at least one expected frequency in said FSK signal; integrating said correlation over an interval; if a signal is present, based on a thresholding of a result of said integrating, generating a validation signal; and outputting said validation signal."

It is submitted that, since these limitations found in amended independent Claims 1 and 31 are not taught by the cited art, these claims are patentable.

As noted above, Atkinson teaches a security device which transmits data from a sending host (hostA) to a receiving host (hostB), in order to authenticate the validity of the sending host (hostA). This is different from authentication of a user (amended Claim 1) and "generating a validation signal" for a user (amended Claim 31), which are not taught in the patent to Atkinson.

Daudelin teaches an FSK demodulator. Daudelin does not teach authentication/validation of a user as recited in amended Claims 1 and 31.

While the Examiner has stated that, since encryption coding is a well-known practice, "the skilled person would have been motivated to use such algorithm to communicate efficiently and securely in a distributed environment," the Examiner has produced no prior art reference that teaches authenticating the use of an authentication device by at least a first user, as recited in amended Claim 1.

Applicant respectfully submits, therefore, that amended independent Claim 1 is patentable over Atkinson in view of Daudelin. It is further submitted that Claims 9-16 are allowable, as they depend from allowable amended independent Claim 1.

Additionally, while the Examiner has stated that it would have been obvious to one skilled in the art "to want to have a hacker-proof authentication by using mechanism of transmission of data using frequency shift key," the Examiner has produced no prior art reference that teaches "receiving an acoustic signal from at least a first user;...generating a validation signal; and...outputting said validation signal," as recited in amended Claim 31.

In view of the foregoing discussion, it is submitted that amended independent Claim 31 is patentable over Atkinson in view of Daudelin. It is further submitted that Claims 32-36 are patentable, as they depend from allowable amended independent Claim 31.

All of the issues raised by the Examiner have been dealt with. In view of the foregoing, it is submitted that all the claims now pending in the application are allowable. An early Notice of Allowance is therefore respectfully requested.

Respectfully submitted,



Martin D. Moynihan
Registration No. 40,338

Date: June 8, 2009

Enclosures:

- Petition for Extension (Two Months)
- Additional Claims Transmittal Fee
- Appendix

APPENDIX - FIG. 3

U.S. Patent

Apr. 23, 1996

Sheet 3 of 4

5,511,122

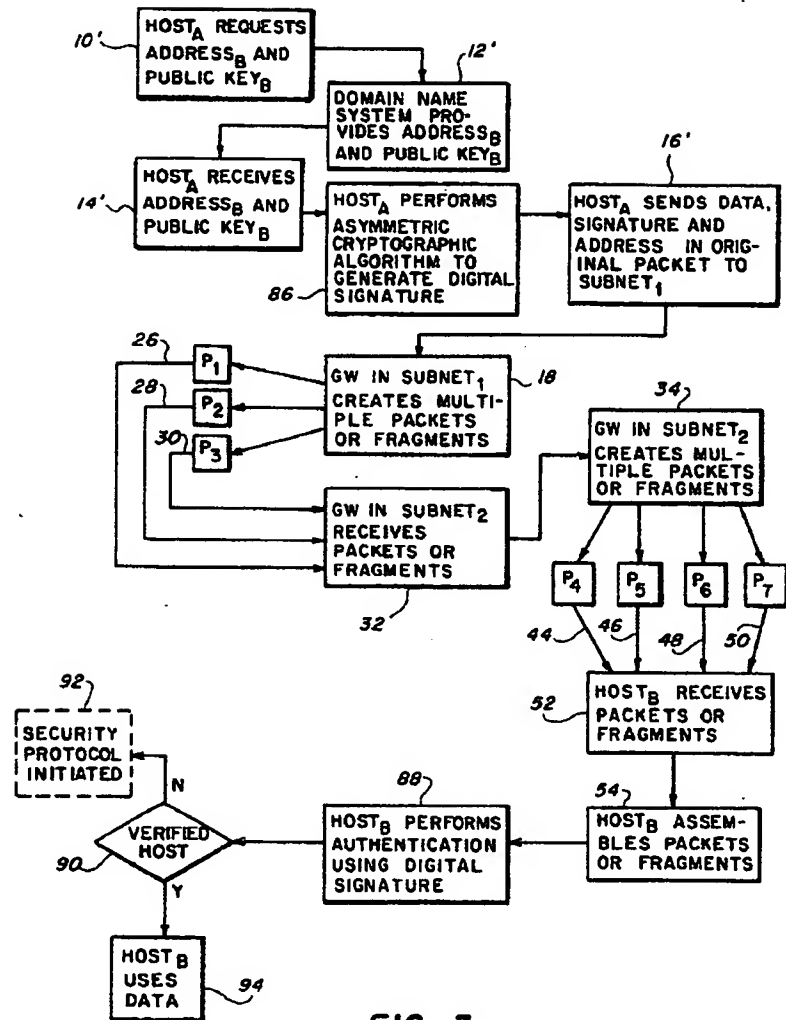


FIG. 3

APPENDIX - FIG. 4

U.S. Patent

Apr. 23, 1996

Sheet 4 of 4

5,511,122

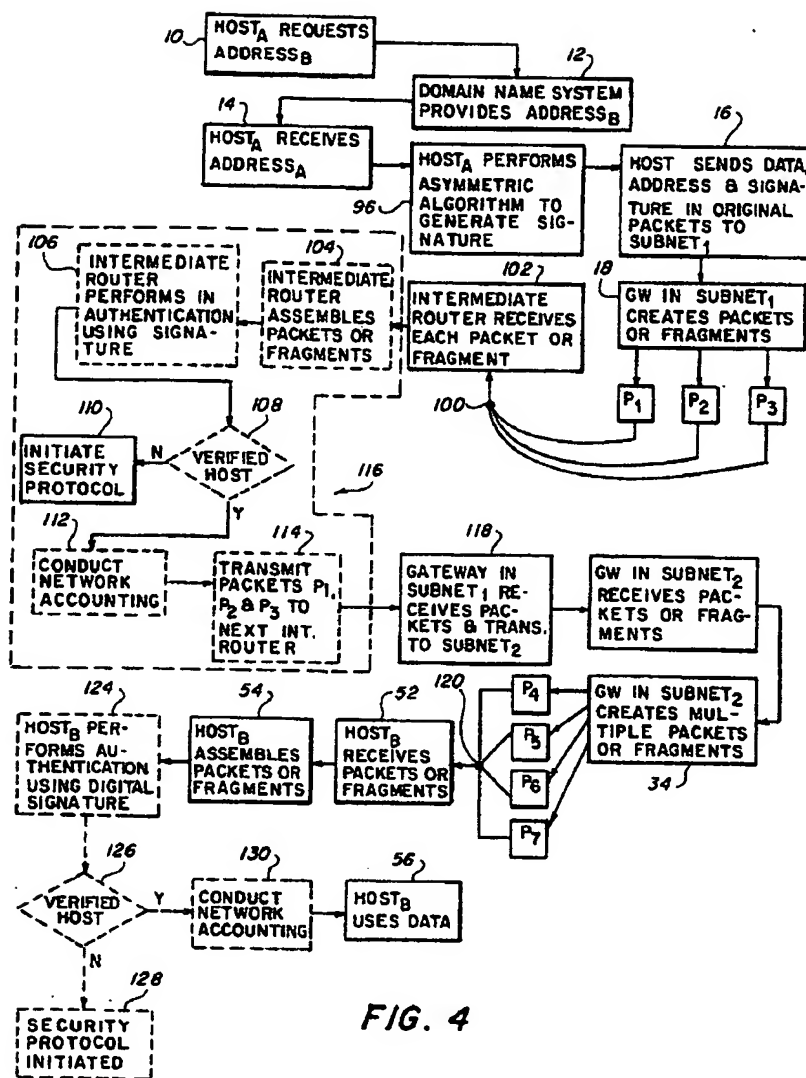


FIG. 4